*****Draft – for Review and Comment*****

Corporate Information Security Working Group
Adam H. Putnam, Chairman

Subcommittee on Technology, Information Policy, Intergovernmental Relations & the Census

Government Reform Committee, U.S. House of Representatives

Report of the Best Practices and Metrics Teams

September 15, 2004

*****Draft – for Review and Comment*****
Information Security Program Elements and Supporting Metrics

Background

During Phase I of the Corporate Information Security Working Group (CISWG) convened in November 2003 by Adam Putnam, (R) Fla., the Best Practices team surveyed available information security guidance. It concluded in its March 2004 report[1] that much of this guidance is expressed at a relatively high level of abstraction and is therefore not immediately useful as actionable guidance without significant and often costly elaboration. A one-page listing of Information Security Program Elements regarded as essential content for comprehensive enterprise management of information security was created, upon which it was hoped a structure of actionable guidance could be built for use by a wide variety of organizations.

The Best Practices and Metrics teams of CISWG Phase II, convened in June 2004, were charged with expanding on the work of Phase I by refining the Information Security Program Elements and developing Metrics supporting each of the elements. The goal was to develop a resource that would help Board members, managers, and technical staff, establish a comprehensive structure of principles, policies, processes, and performance metrics to support the people, process, and technology aspects of information security.

This draft document represents the work of the CISWG Phase II Best Practices and Metrics Teams (CISWG team rosters are below). We solicit your review and comment. We would be most grateful for your feedback on the contents of this document as to its usefulness in the enterprise setting for organizing and monitoring an information security program.

Please email your comments to Clint Kreitner (ckreitner@cisecurity.org) by October 6. We thank you in advance for your helpful assistance in this important endeavor.

Introduction

It is imperative that public and private sector organizations protect the information entrusted to them by various stakeholders against unauthorized access, disclosure, use, or damage. Not only is this a basic fiduciary responsibility, but a growing body of external requirements mandates attention to information security. U.S. federal government agencies must demonstrate compliance with FISMA. Private sector organizations are subject to the information security implications of HIPAA, Gramm-Leach-Bliley, and Sarbanes-Oxley.

The primary responsibility for information security resides with the Board of Directors/Trustees in its role as keeper of the governance framework. Protecting information involves implementing information security principles, policies, and processes, plus performance and compliance metrics that support that framework.

The term “information” as used here includes information in human, physical, and electronic forms. Some information can be considered critical to the organization’s success, such as that relating to products, processes, finance, customers, and copyrighted or patented intellectual property. Loss or compromise of certain information can be harmful or even fatal to an organization, in terms of damage to its reputation, financial status, or its operational ability to function.

Basic fiduciary responsibilities include protection of shareholder interests, compliance with external requirements, and conduct of internal and external audits, all of which have information security implications. A balanced Information Security Program embraces a carefully selected set of foundational principles such as the guidelines promulgated by the Organization for

Economic Cooperation & Development[2], or the Generally Accepted Information Security Pervasive Principles[3]. The Board should adopt a set of basic principles on which management can build a structure of security policies, processes, and controls.

Effective management of information security typically involves reaching into all areas of the enterprise with special attention to critical assets and operational functions. Consequently, close collaboration among Board members and executive managers is essential. Generally, the first step is to identify and list information assets, properly classified with respect to confidentiality, integrity, availability, and privacy considerations. The same should be done for objectives and functions that are dependent upon information security.

A risk assessment considering vulnerabilities, probabilities, and impact, should be conducted to enumerate the risks to which the information assets, objectives, and functions are exposed. After understanding the risks, strategies can be defined and implemented to mitigate those risks. Recognizing that total risk elimination is impossible, it is important for the Board to establish tolerable thresholds for known risks. This enables the Board to convey its level of tolerance for various risks to executive management in a meaningful way.

Equally important is for the Board to make a clear assignment of senior information security management roles, responsibilities, and accountabilities, plus provide appropriate enabling resources. Likewise, executive management should make clear assignments of information security roles and responsibilities throughout the organization. Care should be taken to ensure the people assigned information security responsibilities possess the skills and certifications appropriate for their assignment. Some information security knowledge is highly specialized and technical, some is managerial, and some involves general information security awareness and skills appropriate for everyone in the organization. Ideally, all employee job descriptions should include a clear definition of information security and privacy responsibilities and information security knowledge requirements. A record should be kept of employees' written acknowledgement of their responsibilities for privacy, protection of information, and acceptable use policies.

A popular dictum states “What gets measured gets done”. When a Board of Directors requires the CEO to regularly report values of specified metrics, the CEO thereby knows what the directors consider important. Likewise, when a CEO requires the managers to regularly report values of certain metrics, those managers know what is important to the CEO. It is up to the Board and executive management to articulate metrics supporting the elements of the Information Security Program. In the technology realm, it is important that technical configurations and controls support policies established by management.

Metrics are about transforming policy into action and measuring performance. Visible metric scores provide a positive influence on human behavior by invoking the desire to succeed and compare favorably with one’s peers. Metrics report how well policies and processes are functioning, and whether or not desired performance outcomes are being achieved.

The Information Security Program Elements and Supporting Metrics described below are intended to help those in authority ensure that appropriate steps have been taken to protect the organization’s critical information assets plus the information supporting its key objectives and functions.

Although they are intended to be relatively generic, these Information Security Program Elements and Supporting Metrics are not offered on a “One size fits all” basis. It is assumed that

each organization will thoughtfully consider which Information Security Program Elements and which Supporting Metrics might be helpful in its own circumstances. The suggested metrics are subject to local modification and supplementation as desired.

From a legal perspective, the sensitivity of the information gathered and documented through the use of the suggested metrics is recognized. Further, there is a cost involved in implementing these recommendations in terms of executive and employee time, and financial resources. As with any approach designed to manage risk, each organization must conduct its own cost benefit analysis and decide on the applicability of the guidance contained in this document to its internal information security program. During litigation, the discoverability of documented security weaknesses can result in legal liability in the US. Exposure to privacy law liability in the EU and elsewhere may impose limitations on the documentation of employee policy violations.

The goal of this document is to provide practical and operationally actionable guidance to organizations while remaining mindful of the disparate needs of different organizations. It is hoped that it will serve as a useful resource for organizations seeking to initiate or enhance an information security program designed to protect the enterprise from financial, functional, or reputational damage resulting from unauthorized access, disclosure or use of the information entrusted to it by its stakeholders.

The following CISWG Phase II Team members participated in the development of this document:

Information Security Best Practices & Guiding Principles Team

- **Clint Kreitner- Center for Internet Security Coordinator**
- **Michael Dickson- AICPA Coordinator**
- **Leslie Saul Garvin- TechNet**
- **Karyn Waller- AICPA**
- **Jim Kohlenberger/Dexter Ingram/Robert Tai- Business Software Alliance**
- **Brett Kilbourne- United Telecom Council**
- **Michael Rasmussen- Forrester Research**
- **John Carlson- The Financial Services Roundtable/BITS**
- **Emily Frye- Critical Infrastructure Protection Project**
- **Mark Silver- The Business Roundtable**
- **Robert Daniels- ISSA**

Adjunct Members

Phil Campbell – Sandia Labs
Julia Allen – Carnegie Mellon University/SEI
Jack Suess – University of Maryland
Charlie LeGrand – Institute of Internal Auditors
Chrisan Herrod – Securities & Exchange Commission
Adam Stone - Fortis
Rodney Petersen -- Educause
Don Holden - Consultant
Michael Hines – Purdue University

*****Draft – for Review and Comment*****

Information Security Program Elements and Supporting Metrics

Performance Metrics, Reporting & Information Sharing Team

- **Charlie Le Grand- Institute of Internal Auditors Coordinator**
- **Clint Kreitner- Center for Internet Security Coordinator**
- **Alan Paller- The SANS Institute**
- **Paul Kurtz- Cyber Security Industry Alliance**
- **Cristin Flynn/Maggie Mansourkia - U. S. Internet Service Provider Association**
- **Jim Lewis- Center for Strategic & International Studies**
- **Michael Rasmussen- Forrester Research**

Adjunct Members

Phil Campbell – Sandia Labs
Mike Dickson - AICPA
Karyn Waller – AICPA
Don Holden - Consultant
Dan Daly – Subcommittee staff
Michael Hines – Purdue University
Susan Kennedy – Univ. of Pennsylvania
Julia Allen – Carnegie Mellon Univ/SEI
Chrisan Herrod – Securities & Exchange Commission

*****Draft – for Review and Comment*****

Information Security Program Elements

Governance (Board of Directors/Trustees):

1. Establish Risk Thresholds for Critical Information Assets and Information-dependent Functions and Objectives (ISPE1)
2. Establish Broad Information Security Program Principles and Assign Senior Management Accountabilities for Information Security (ISPE2)
3. Protect Stakeholder Interests Dependent on Information Security (ISPE3)
4. Ensure Appropriate Information Security Requirements for Strategic Partners and Vendors (ISPE4)
5. Comply with External Information Security Requirements (e.g. Sarbanes-Oxley, HIPAA, GLB) (ISPE5)
6. Establish Requirements for Internal and External Audits of the Information Security Program (ISPE6)
7. Specify the Information Security Metrics to be Reported to the Board (ISPE7)

Management

8. Establish Information Security Management Policies and Controls and Monitor Compliance (ISPE8)
9. Assign Information Security Roles, Responsibilities, Required Skills, and Enforce Role-based Information Access Privileges (ISPE9)
10. Assess Information Risks & Actively Manage Risk Mitigation (ISPE10)
11. Ensure Implementation of Information Security Requirements for Strategic Partners and Vendors (ISPE11)
12. Identify and Classify Information Assets (ISPE12)
13. Ensure Business Continuity (ISPE13)
14. Approve Information Systems Architecture during Acquisition, Development, Operations, and Maintenance (ISPE14)
15. Protect the Physical Environment (ISPE15)
16. Ensure Internal and External Audits of the Information Security Program with Timely Follow-up (ISPE16)
17. Specify the Information Security Metrics to be Reported to Management (ISPE17)

Technical

18. User Identification and Authentication (ISPE18)
19. User Account Management (ISPE19)
20. User Privileges (ISPE20)
21. Configuration Management (ISPE21)
22. Event and Activity Logging and Monitoring (ISPE22)
23. Communications, Email, and Remote Access Security (ISPE23)
24. Malicious Code Protection, Including Viruses, Worms, and Trojans (ISPE24)
25. Software Change Management, including Patching (ISPE25)
26. Firewalls (ISPE26)
27. Data Encryption (ISPE27)
28. Backup and Recovery (ISPE28)
29. Incident and Vulnerability Detection and Response (ISPE29)
30. Specify the Technical Metrics to be Reported to Management (ISPE30)

Information Security Program Elements and Supporting Metrics for Boards of Directors/Trustees

Establishing a competent Information Security Program requires that Board members devote attention to the following program elements:

1. **Establish Risk Thresholds for Critical Information Assets and Information-dependent Functions and Objectives**
2. **Establish Broad Information Security Program Principles and Assign Senior Management Accountabilities for Information Security**
3. **Protect Stakeholder Interests Dependent on Information Security**
4. **Ensure Appropriate Information Security Requirements for Strategic Partners and Vendors**
5. **Comply with External Information Security Requirements (e.g. Sarbanes-Oxley, HIPAA, GLB)**
6. **Establish Requirements for Internal and External Audits of the Information Security Program**
7. **Specify the Information Security Metrics to be Reported to the Board**

Below is a list of metrics suggested for Board use in connection with its information security responsibilities. Desired target values for each of the metrics will generally be self-evident as to whether higher or lower is better.

1. **Establish Risk Thresholds for Critical Information Assets and Information-dependent Functions and Objectives**

   1.1. ***Percentage of key information <u>assets</u> for which a comprehensive strategy has been implemented to reduce information security risks to acceptable thresholds***

   1.2. ***Percentage of significant or material organizational <u>objectives</u> for which a comprehensive strategy has been implemented to reduce information security risks to acceptable thresholds***

   1.3. ***Percentage of key organizational <u>functions</u> for which a comprehensive strategy has been implemented to reduce information security risks to acceptable thresholds***

   <u>Note</u>: Metrics 1.1, 1.2, & 1.3 involve several implicit assumptions about what the Board and executive management should do in designing and implementing an Information Security Program, the extent of which will be influenced by the size and complexity of the organization.

   - First, explicitly identify information assets, plus information-dependent objectives (goals, plans), and functions that are critical to the success of the organization.
   - Second, assess the risks to which this information is potentially exposed, with respect to confidentiality, integrity, availability, and privacy.
   - Third, establish acceptable thresholds for those risks.
   - Fourth, identify and implement information security strategies, policies, and methods involving people, process, and technology to mitigate known risks to acceptable levels.

2. Establish Broad Information Security Program Principles and Assign Senior Management Accountabilities for Information Security

2.1. ***Percentage of Information Security Program Principles for which policies and controls have been fully implemented by management***

Note: The Board will likely want this metric to be reported for selected components of the organization responsible for critical information assets, objectives, or functions

2.2. ***Percentage of senior management information security roles for which responsibilities, accountabilities, and authority have been assigned***

Note: Capable management is a critical element of the Information Security Program. The Board should carefully define and assign senior information security management roles, responsibilities, and accountabilities.

2.3. ***Percentage of information security management employees who have been deemed by responsible authority to possess the information security knowledge, skills and certifications appropriate for their position***

Note: It is crucial to ensure that key information security managers and others in the organization possess the information security knowledge and skills appropriate for their assignment. A number of organizations award certifications that can serve as an indicator of the information security knowledge and experience possessed by a particular person. Available certifications include: ISC^2's CISSP; ISACA's CISA and CISM; and the SANS Institute's GIAC certifications for various technologies. There are many others.

3. Protect Stakeholder Interests Dependent on Information Security

3.1. ***Percentage of security incidents that caused damage beyond established risk thresholds to the organization's assets, objectives, or functions***

Note: All organizations experience security incidents where unauthorized access to information is attempted or achieved. Tracking the number of incidents that cause damage in relation to established risk thresholds as a percentage of the total number of incidents is a useful indication of both the ultimate effectiveness of the organization's Information Security Program, as well as the overall magnitude of incident activity. Analysis of the types of damage incurred will help devise improved defenses.

4. Ensure Appropriate Information Security Requirements for Strategic Partners and Vendors

4.1. ***Percentage of strategic partner and vendor relationships for which information security requirements have been implemented***

Note*:* For the security of their own information, organizations often depend heavily on strategic partners and vendors, particularly technology vendors, and therefore should require them to demonstrate compliance with key requirements of the Information Security Program.

5. Comply with External Information Security Requirements (e.g. Sarbanes-Oxley, HIPAA, GLB)

5.1. ***Percentage of key external requirements for which the organization has been deemed by objective audit to be in compliance***

Note: Various external requirements have different levels of significance or materiality to the organization, so it is important to understand the relative level of risk or impact represented by each external requirement with which the organization is out of compliance.

6. Establish Requirements for Internal and External Audits of the Information Security Program

6.1. ***Percentage of required internal and external audits completed and reviewed by the Board***

Note: Internal and external audit review information should be broken out by business process/function so the risk to that part of the organization is clearly identified. Audit findings should be ranked in order of significance/materiality so the risk and impact they represent can be better understood. Management's response to audit findings in the form of planned action should be properly documented.

6.2. ***Percentage of audit findings that have been corrected***

Note: This will give visibility to progress being made in implementing corrective actions related to audit findings.

7. Specify the Information Security Metrics to be Reported to the Board

Note: A carefully chosen set of information security metrics for management reports of information security status to the board will clarify to management what the board members consider important and on which they wish to be kept informed. Board members can choose their information security metrics from those defined above and/or create others they consider appropriate for the organization. For large enterprises, it is assumed the metrics will be calculated by various units of the organization and aggregated at various levels up to the entire enterprise. Each metric is reported for the current and last 'n' reporting periods so that trends and changes are visible (such as n=3 if quarterly reports are generated, to provide an annual perspective). For percentage metrics, the numerator and denominator as well as the resulting percentage, should be reported. Reporting frequency and target values for the chosen metrics should be specified by the Board.

*****Draft – for Review and Comment*****

Information Security Program Elements and Supporting Metrics for Management

The following is intended to help managers implement the information security goals and policies established by the Board. Establishing a competent Information Security Program requires management to devote attention to the following program elements:

8. **Establish Information Security Management Policies and Controls and Monitor Compliance**
9. **Assign Information Security Roles, Responsibilities, Required Skills, and Role-based Information Access Privileges**
10. **Assess Information Risks & Actively Manage Risk Mitigation**
11. **Ensure Implementation of Information Security Requirements for Strategic Partners and Vendors**
12. **Identify and Classify Information Assets**
13. **Ensure Business Continuity**
14. **Approve Information Systems Architecture during Acquisition, Development, Operations, and Maintenance**
15. **Protect the Physical Environment**
16. **Ensure Internal and External Audits of the Information Security Program with Timely Follow-up**
17. **Specify the Information Security Metrics to be Reported to Management**

Below is a list of metrics suggested for management use in connection with its information security responsibilities. Desired target values for each of the metrics will generally be self-evident as to whether higher or lower is better.

8. **Establish Information Security Management Policies and Controls and Monitor Compliance**

8.1. ***Percentage of Information Security Program Elements for which policies have been developed and implemented***

Note: As a minimum, the overall information security policy structure and content should include the topics represented by the Information Security Program Elements defined in this document. It is also important for management to establish specific policies for the Technical Information Security Program Elements on topics such as encryption, event and activity logging, user identification and authentication, configuration management, and others.

8.2. ***Percentage of information security management policies approved and monitored by senior management and board of directors/trustees in accordance with policy***

8.3. ***Percentage of information security controls approved by senior management and monitored by senior management and board of directors/trustees in accordance with policy***

8.4. ***Percentage of staff assigned responsibilities for information security policies who have acknowledged accountability for their responsibilities in connection with those policies***

8.5. ***Number of information security policy violations***

8.6. ***Percentage of business unit heads and senior managers who have specific programs in place to ensure compliance with information security policies and controls***

9. Assign Information Security Roles, Responsibilities, Required Skills, and Enforce Role-based Information Access Privileges

Note: This element defines and assigns all information security roles and responsibilities and describes the skills necessary to fulfill these. In addition, this element reviews and enforces role-based access privileges assigned to each information asset or class of asset as identified in Program Element12.

9.1. ***Percentage of position descriptions that define the information security roles, responsibilities, skills, and certifications for:***

- ***a. Security Managers and Administrators***
- ***b. IT personnel***
- ***c. General staff system users***

9.2. ***Percentage of job performance reviews that include evaluation of information security responsibilities and information security policy compliance***

9.3. ***Percentage of systems and applications that comply with the separation of duties principle***

9.4. ***Number of users with access to security software who are not security administrators***

9.5. ***Number of users who are able to assign security privileges for systems and applications who are not security administrators***

9.6. ***Percentage of users whose access privileges have been reviewed this reporting period***

- ***a. Employees with high level system privileges***
- ***b. All other employees***
- ***c. Contractors***
- ***d. Vendors***
- ***e. Others***

9.7. ***Percentage of users with high level system privileges who have undergone background checks***

9.8. ***Percentage of annual turnover of people in key information security roles***

10. Assess Information Risks & Actively Manage Risk Mitigation

10.1. ***Percentage of critical information assets and information-dependent functions and objectives for which formal risk assessments have been performed and documented as required by policy***

10.2. ***Percentage of critical assets and functions for which the cost of compromise (loss, damage, disclosure, disruption in access to) has been quantified***

Note: Costs of compromise include violations of confidentiality, availability, integrity, and privacy considerations.

10.3. ***Percentage of identified risks that have a defined risk mitigation plan against which status is reported in accordance with policy***

11. Ensure Implementation of Information Security Requirements for Strategic Partners and Vendors

11.1. ***Percentage of known information security risks that are related to strategic partner or vendor relationships***

11.2. ***Percentage of critical information assets or functions to which strategic partner or vendor personnel have been given access***

11.3. ***Percentage of strategic partner and vendor personnel with current information access privileges who have been reviewed by designated authority to have continued need for access in accordance with policy***

11.4. ***Percentage of systems with critical information assets or functions that are electronically connected with vendor or partner systems***

11.5. ***Percentage of security incidents that involved strategic partner or vendor personnel***

11.6. ***Percentage of strategic partner/vendor agreements that include/demonstrate external verification of policies and procedures***

11.7. ***Percentage of strategic partner and vendor relationships that have been reviewed for compliance with information security requirements***

11.8. ***Percentage of out-of-compliance review findings that have been corrected since the last review***

12. Identify and Classify Information Assets

12.1. ***Percentage of information assets that have been reviewed and classified in accordance with the classification scheme established by policy***

12.2. ***Percentage of information assets that have been assigned a priority in accordance with the most recent risk assessment***

Note: Not all information assets can be protected at the highest level. Protection decisions and corresponding investments need to be based on an assessment of risk to the asset, the asset's value, the impact if the asset is compromised (lost, damaged, disclosed, access disrupted), and a comparison of the cost to reconstitute the asset vs. the cost to protect the asset.

12.3. ***Percentage of information assets for which dollar values have been quantified***

12.4. ***Percentage of information assets for which the key stakeholder (owner, custodians) has been identified***

12.5. ***Percentage of information assets with defined access privileges that have been assigned based on role and in accordance with policy***

Note: The identification and classification of any information asset needs to include access privileges to that asset (create, read, write, edit/modify, delete, etc.). Such privileges need to be assigned to specific roles within the organization as identified in Program Element 9.

12.6. ***Date when the asset inventory was last updated***

Note: This metric assumes the existence of a full asset inventory that is regularly updated based on events (such as the addition or retirement of critical information assets) or periodically such as quarterly.

13. Ensure Business Continuity

Note: Business continuity includes crisis management, disaster recovery, and incident management. The term "business continuity plan" encompasses plans for all of these functions and their supporting processes.

Note: Incident management includes prevention, preparation, detection, response, recovery/restoration, and improvement. The Incident Management Plan includes vulnerability assessment and management of at least systems on which critical information assets reside and that support critical information-dependent functions and objectives.

13.1. ***Percentage of organizational units with a documented business continuity plan for which specific responsibilities have been assigned***

13.2. ***Percentage of business continuity plans that have been reviewed, exercised/tested, and updated in accordance with policy***

13.3. ***Percentage of critical information assets with an established backup frequency and where the ability to restore from backups has been exercised/tested in accordance with policy***

13.4. ***Number of successful attacks (defined as those that cause damage to critical assets and functions beyond acceptable risk thresholds) for each of the past four reporting periods***

13.5. ***Estimated damage or loss in dollars resulting from all successful attacks in each of the past four reporting periods***

Note: Consider staff time, lost transactions/business, lost customers, system and service downtime, etc., when calculating loss. The availability of aggregate losses for all successful attacks implies that data for individual attacks is also available.

14. Approve Information Systems Architecture during Acquisition, Development, Operations, and Maintenance

Note: This element applies to review and approval of the information systems architecture for compliance with information security requirements and policies, and for any impacts to information security during the architecture's life cycle.

14.1. ***Percentage of information security risks identified in the most recent risk assessment that have been adequately mitigated by the approved systems architecture***

14.2. ***Percentage of system architecture changes (additions, modifications, or deletions) that were reviewed for security impacts, approved by appropriate authority, and documented via change request forms***

14.3. ***Percentage of security reviews/audits of system architecture required by policy that were conducted and reviewed, with appropriate follow-up***

14.4. ***Percentage of critical information assets or functions residing on systems that are currently out of compliance with the approved systems architecture***

15. Protect the Physical Environment

15.1. ***Percentage of critical organizational information assets and functions that have been reviewed from the perspective of physical risks such as controlling physical access and physical protection of backup media***

15.2. ***Percentage of critical organizational information assets and functions exposed to physical risks for which risk mitigation actions have been implemented***

15.3. ***Percentage of critical assets that have been reviewed from the perspective of environmental risks such as temperature, fire, flooding, etc.***

15.4. ***Percentage of personnel assigned to provide physical security who have been trained and deemed to be qualified to carry out their responsibilities***

15.5. ***Percentage of servers in locations with controlled physical access***

16. Ensure Regular Internal and External Audits of the Information Security Program with Timely Follow-up

16.1. ***Percentage of information security requirements from applicable laws and regulations that are included in the internal/external audit program and schedule***

16.2. ***Percentage of information security audits conducted in compliance with the approved internal/external audit program and schedule***

16.3. ***Percentage of management actions in response to audit findings / recommendations that were implemented as agreed as to timeliness and completeness***

17. Specify the Information Security Metrics to be Reported to Management

Note: A carefully chosen set of information security metrics for reports to management of information security status will clarify to operational units what management considers important and the topics on which management wishes to be kept informed. Management can choose its set of information security metrics from those defined above and/or create others considered appropriate for the organization. For large enterprises, it is assumed the metrics will be calculated by various units of the organization and aggregated at various levels up to the entire enterprise. Each metric is reported for the current and last 'n' reporting periods so trends and changes are visible (such as n=3 if quarterly reports are generated, to provide an annual perspective). For percentage metrics, the numerator and denominator as well as the resulting percentage, should be reported. Reporting frequency and target values for the management metrics should be specified by management as part of its Information Security Program policies.

Information Security Program Elements and Supporting Metrics – Technical

Technical controls are those controls contained within and executed by the various information technology environments such as Microsoft Windows, Sun Solaris, Linux, Cisco Router IOS, etc. For each of the Technical Program Elements, multiple technical controls are commonly available within each of the various technologies.

Many, if not most, of an organization's information security policies will ultimately be implemented by assigning values to technical security controls within the various information technology environments. For example, it is common to set a technical control for automatically logging off active user sessions on idle workstations after a certain number of minutes. The policy value for a technical control such as this is generally established by adopting a recognized standard such as the Center for Internet Security consensus benchmarks[4], and then making local adaptations as appropriate. The ability to automate technical controls that implement and demonstrate compliance with certain information security policies represents a powerful security resource that a security-conscious organization can use to its benefit.

Establishing a complete Information Security Program requires attention to the following technical program elements:

18. User Identification and Authentication
19. User Account Management
20. User Privileges
21. Configuration Management
22. Event and Activity Logging and Monitoring
23. Communications, Email, and Remote Access Security
24. Malicious Code Protection
25. Software Change Management, including Patching
26. Firewalls
27. Data Encryption
28. Backup and Recovery
29. Incident and Vulnerability Detection and Response
30. Specify the Technical Metrics to be Reported to Management

The metrics defined herein represent a minimum baseline and are therefore not exhaustive. The technical program element metrics chosen by a particular organization are influenced by the perceived risks and associated information security principles and policies adopted and promulgated by its governing board and management. The controls of value to various organizations will vary according to size and complexity, the specific risks being mitigated, the efficacy attributed to certain controls, and available technical security expertise.

18. User Identification and Authentication

18.1. ***Percentage of active user ID's assigned to only one person***

18.2. ***Percentage of systems and applications that perform password policy verification***

18.3. ***Percentage of active user passwords that are set to expire in accordance with policy***

18.4. ***Percentage of systems with critical information assets that use stronger authentication than ID's and passwords in accordance with policy***

Note: So called three-factor authentication requires something you know (a user ID, password, or PIN), something you have (a security device you plug into a USB port), and something you are (a retina scan or fingerprint).

19. User Account Management

19.1. ***Percentage of systems where vendor-supplied accounts and passwords have been disabled or reset***

Note: Systems often come with vendor-supplied accounts such as guest accounts and vendor-supplied passwords for administrator accounts. In general, vendor-supplied accounts should be disabled and vendor-supplied passwords should be changed, since they are generally widely known.

19.2. ***Percentage of active user accounts assigned to personnel who have left the organization or no longer have need for access***

19.3. ***Percentage of systems with account lockout parameters set in accordance with policy***

19.4. ***Percentage of inactive user accounts that have been disabled in accordance with policy***

19.5. ***Percentage of workstations with session time-out/automatic logout controls set in accordance with policy***

Note: Analysis of illegal insider activity has shown that leaving a workstation unattended that is logged into a user account is an invitation to inappropriate access by persons other than the one to whom the user account is assigned. Automatic log-off is an example of how an automated technical control can be used to enforce organizational policy (in this case, session control policy) on a real-time basis.

20. User Privileges

20.1. ***Percentage of active user accounts that have been reviewed for justification of current access privileges in accordance with policy***

20.2. ***Percentage of systems where permission to install non-standard software is limited in accordance with policy***

Note: Unauthorized installation of non-approved software is one way malicious software (viruses, Trojans, and worms) finds it way onto an organization's systems. Accordingly, a policy of discipline based on the following security principles is considered baseline security practice. First, users should not have administrative access or control over organization-owned systems. Second, the only software authorized for procurement is that which is included in the organization's approved software suite. Third, only persons authorized by management are allowed to install that software on the organization's systems. Fourth, exceptions to the above policies based on a valid business case can be authorized on a case basis by designated management.

20.3. ***Percentage of systems and applications where assignment of user privileges is in compliance with the policy that specifies role-based information access privileges***

21. Configuration Management

21.1. ***Percentage of systems for which configuration settings have been implemented as required by policy***

21.2. ***Number of deviations from approved system configurations***

Note: Management should establish specific approved system configurations as policy for each operating system environment. The approved configurations will generally be based on a recognized standard of practice and some degree of local deviation that may be justified by operational necessity. The number of deviations from approved configurations should be kept to a minimum via a waiver process.

21.3. ***Percentage of systems that are continuously monitored for configuration policy compliance with out-of-compliance alarms or reports***

21.4. ***Percentage of systems whose configuration is compared with a previously established trusted baseline in accordance with policy***

Note: One of the most effective ways to ensure malicious code has not been inadvertently installed on a running system is to periodically compare its entire 'footprint' or configuration with a previously established trusted baseline that is stored in a secure location. This comparison can reveal the presence of unexpected files or changes to files that can then be analyzed further. The trusted baseline is updated when the configuration incorporates authorized changes.

21.5. ***Percentage of systems where the authority to make configuration changes is limited in accordance with policy***

21.6. ***Percentage of systems where the services deemed to be unneeded have been disabled***

22. Event and Activity Logging and Monitoring

22.1. ***Percentage of systems for which event and activity logging has been implemented in accordance with policy***

22.2. ***Percentage of systems for which event and activity logs are monitored and reviewed in accordance with policy***

22.3. ***Percentage of systems for which log size and retention duration have been implemented in accordance with policy***

22.4. ***Percentage of systems that generate warnings about anomalous or potentially unauthorized activity based on review of log data***

23. Communications, Email, and Remote Access Security

23.1. ***Percentage of notebooks and mobile devices that are required to verify compliance with approved configuration policy prior to being granted network access***

Note: When they connect to the enterprise network, notebooks and other mobile devices not properly configured and protected with anti-virus, personal firewall, intrusion detection and integrity checking software can introduce malicious software (viruses, worms, and Trojan horses) into the network. Before being granted network access, such devices should be automatically checked by a software utility to ensure they are using the security protections required by policy.

23.2. ***Percentage of communications channels using secure transmissions***

Note: When sensitive information is sent as email, file transfer, web pages (HTML), or instant messaging over the Internet and other unprotected links, it is possible for someone other than the intended receiver to see the information. Communications can be protected by using secure versions of email that authenticate the receiver and encrypt the contents. Web pages can be protected with SSL/TLS and password-based authentication of client users. Virtual private networks that use IPSEC or web-based SSL/TLS will secure communications involving transactions, file transfers, etc. Alternatively a general encryption utility can be used to encrypt a sensitive file before sending the file using regular email, instant messaging, or FTP. Security policy should describe what information requires protection when sent over an open network such as the Internet and the appropriate security mechanism to be used.

23.3. ***Percentage of communications filtered for inappropriate content, intellectual property content, viruses, Trojans, and spam***

Note: Incoming communications such as email can contain malicious code (viruses, worms, Trojan horses). This malicious code may be encrypted making it difficult to detect at a central server. Therefore, a check should be made at both the server and the user's computer where encrypted or otherwise hidden malicious code can be detected and eliminated. In addition, filters for inappropriate material such as music files, pornography, and spam should be checked both on incoming and outgoing communications. Outbound communications should also be checked for malicious code and unauthorized sending of sensitive information such as financial or personnel data, trade secrets, and other electronic intellectual property.

23.4. ***Percentage of host servers that are protected from becoming relay hosts***

Note: Spammers look for unprotected email servers they can use to forward spam mail. They also look for other servers where they can install mail relay software to relay their spam mail. In addition to using your network resources, the spam coming from your Internet address can damage your reputation and result in other organizations blocking all mail from your address. Email servers should restrict relaying from external sources.

23.5. ***Percentage of mobile users who access enterprise facilities using secure communications methods***

Note: Remote users who use unprotected access when connecting to an organizational network, risk disclosing user ID and passwords as well as sensitive company information. When users access the organization over an open network they should use a secure connection such as a virtual private network (VPN) using SSL/TLS or IPSEC or a secure web based session (SSL/TLS). Wireless users should

use WEP or preferably WPA to protect against disclosure. IEEE 802.1x should be considered for authenticating both wireless and wired remote users.

24. Malicious Code Protection, Including Viruses, Worms, and Trojans

24.1. ***Percentage of workstations (including notebooks) with automatic protection in accordance with policy***

24.2. ***Percentage of servers with automatic protection in accordance with policy***

24.3. ***Percentage of mobile devices with automatic protection in accordance with policy***

25. Software Change Management, including Patching

25.1. ***Percentage of systems with the latest available patches installed***

Note: If this metric is not reported as 100%, rationale should be provided as to why particular patches have not been installed. It is advisable to test patches in a non-production environment before operational deployment to identify possible adverse impact on functionality or interoperability of operational software. An organization may make a conscious decision to delay patch deployment or eliminate a patch from deployment consideration. This should be done only after careful consideration of the criticality of the system(s) involved plus the vulnerabilities and risks involved in not deploying the patch.

25.2. ***Mean time from vendor patch availability to patch installation by type of technology environment***

25.3. ***Percentage of software changes that were reviewed for security impacts in advance of installation***

26. Firewalls

26.1. ***Percentage of workstations with personal firewalls installed and configured in accordance with policy***

26.2. ***Percentage of host, sub-network, and perimeter firewalls configured in accordance with policy***

27. Data Encryption

27.1. ***Percentage of critical information assets stored on network accessible devices that are encrypted in accordance with policy***

27.2. ***Percentage of mobile computing devices using encryption for critical information assets in accordance with policy***

27.3. ***Percentage of passwords and PINS that are encrypted (cryptographically one-way hashed) in accordance with policy***

28. Backup and Recovery

28.1. ***Percentage of systems with critical information assets or functions that have been backed up in accordance with policy***

28.2. ***Percentage of systems with critical information assets or functions where restoration from a stored backup has been successfully demonstrated***

28.3. ***Percentage of backup media stored offsite in secure storage***

28.4. ***Percentage of used backup media sanitized prior to reuse or disposal***

28.5. ***Percentage of media libraries that log all media deposits and withdrawals***

29. Incident and Vulnerability Detection and Response

29.1. ***Percentage of operational time that critical services were unavailable (as seen by users and customers) due to security incidents***

Note: Operational time excludes scheduled maintenance and downtime. This metric assumes critical services have been identified as part of a risk assessment.

29.2. ***Percentage of successful attacks (defined as those that cause damage to critical assets and functions beyond acceptable risk thresholds) that exploited existing vulnerabilities with known solutions, patches, or workarounds***

29.3. ***Percentage of systems affected by successful attacks that exploited existing vulnerabilities with known solutions, patches, or workarounds***

29.4. ***Percentage of successful attacks (as defined above) that were managed in accordance with established policies, procedures, and processes***

Note: The intent is to measure the percentage of successful attacks that were handled in accordance with policy, defined procedures, and in-place processes in a disciplined, repeatable, predictable manner. Such behavior assumes the existence of well-defined processes for incident management. This is contrasted with responding to an attack in an ad-hoc, chaotic manner. "Managed" includes detecting an incident, containing an incident and its effects, analyzing the damage caused by an incident and preventing its recurrence, taking corrective action, and restoring services and systems in a timely manner.

29.5. ***Percentage of systems with critical information assets or functions that have been assessed for vulnerabilities in accordance with policy***

29.6. ***Percentage of vulnerability assessment findings that have been addressed since the last reporting period***

30. Specify the Technical Metrics to be Reported to Management

Note: For large enterprises, it is assumed the metrics will be calculated by various units of the organization and aggregated at various levels up to the entire enterprise. Each metric is reported for the current and last 'n' reporting periods so trends and changes are visible (such as n=3 if quarterly reports are generated, to provide an annual perspective). For percentage metrics, the numerator and denominator as well as the resulting percentage, should be reported. Reporting frequency and target values for the technical metrics should be specified by management as part of its Information Security Program policies.

References

[1] http://reform.house.gov/TIPRC/
[2] http://www.oecd.org/document/42/0,2340,en_2649_201185_15582250_1_1_1_1,00.html
[3] http://www.issa.org/gaisp/gaisp.html
[4] http://www.cisecurity.org